UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/694,879	10/29/2003	Martin Zilliacus	27592-00449	4091

30678 7590 02/18/2009

CONNOLLY BOVE LODGE & HUTZ LLP
1875 EYE STREET, N.W.
SUITE 1100
WASHINGTON, DC 20006

EXAMINER	
HOLLIDAY, JAIME MICHELE	
ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
02/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/694,879	ZILLIACUS ET AL.	
	Examiner	Art Unit	
	JAIME M. HOLLIDAY	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,7-14 and 17-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 4, 7-14 and 17-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Arguments

Applicant's arguments filed November 13, 2008 have been fully considered but they are not persuasive.

Applicants state that Examiner noted that the rejection of claims 5, 8, 15, 18, 23 and 32 was in error. Examiner disputes this. Examiner stated that the heading for the 103 (a) rejection as follows "**Claims 1-4, 6, 7, 9-14, 17, 19-22, 24-26, 28, 30-35, 37 and 39 Claims 5, 8, 15, 18, 23 and 32** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Heinonen et al. (U.S. 2003/0112789 A1)** in view of **Hasty, Jr. et al. (US 6,728,232 B2)**, and in further view of **Norefors et al. (US 6,370,380 B1)**," addressing claims 3, 5 and 15 was a typographical error, not that the actual rejections of claims 8, 18, 23 and 32 were in error.

Applicants basically argue that the prior art of record, in particular, the combination of Heinonen et al., Hasty, Jr. et al. and Norefors et al., does not teach or suggest "the code and the wide area identification are to be coupled into a hashed code for proximity identification of the mobile device, and wherein the hashed code is to be transmitted to the mobile device along with an instruction to forward the hashed code to the network server to associate the code and the wide area identification in a subsequent request for service by the mobile device." Further, Applicants argue that there is no teaching or suggestion in Hasty that the hashed MAC address and IP address are for proximity identification of the mobile device, as alleged in the Office Action, but instead, Hasty only discloses that the local ad-hoc table with the hashed IP and MAC addresses are used to answer intercepted ARP and DHCP requests at the

node. Applicants also argue that Norefors does not teach or suggest that the hashed code is forwarded "to the network server to associate the code and the wide area identification in a subsequent request for service by the mobile device," and there is no teaching or suggestion in Norefors of associating the content of the hash code (the code and the wide area identification) in a subsequent request for service by the mobile device.

Examiner respectfully disagrees, because Hasty, Jr. et al. teaches that the MAC address (wide area identification) and class B address (code) are hashed. The Class B address designates the type, location of a node and the network subdivision, which refers to the location/position (proximity) of the node (col. 6 lines 5-15). The combination of Heinonen et al. and Hasty, Jr. et al. does not teach forwarding this hashed code, and the Norefors reference is incorporated to teach this limitation. The claim does not recite what entity receives the request for subsequent service. The handover request to the second access point in Norefors et al. reads on the claimed "subsequent service." Norefors et al. further teach the mobile terminal receiving a message with a hash code and forwarding that message to the second access point for the handover, reading on the claimed "wherein the hashed code is to be transmitted to the mobile device along with an instruction to forward the hashed code to the network server to associate the code and the wide area identification in a subsequent request for service by the mobile device."

Therefore, in view of the preceding arguments, Examiner maintains the previous rejections.

Claim Rejections - 35 USC § 103

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. **Claims 1, 2, 4, 6, 7, 8-14, 17-26, 28, 30-35, 37, 39-52, 54 and 56** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Heinonen et al. (U.S. 2003/0112789 A1)** in view of **Hasty, Jr. et al. (US 6,728,232 B2)**, and in further view of **Norefors et al. (US 6,370,380 B1)**.

Consider **claims 1 and 40**, Heinonen et al. clearly show and disclose that during the period when a mobile wireless device, reading on the claimed "wireless device," is within the coverage area of a short range wireless access point, reading on the claimed "short-range wireless access point [apparatus]," it sends a request for service to be obtained over the Internet from a network server. The short range wireless access point forwards that request over the

Internet to the server, augmented with additional information including the network address and geographic location of the access point. The short range wireless access point receives a response message over the Internet from the server, including a global/local parameter. The global/local parameter will notify the mobile wireless device whether the requested service is available outside the coverage area of the short range wireless access point. The access point forwards the response message to the mobile wireless device, which uses the information in the message to contact the server over the Internet to download web pages or to conduct other server operations. If the user selects to continue the contact with the server, then a stored handover address is accessed. The handover address may be stored in the mobile wireless device or alternately; it may be stored in the short range wireless access point. A cellular telephone connection is made by the mobile wireless device with the regional cellular telephone access point. The Bluetooth access point forwards the response message **435** to the user's Bluetooth device from the server. The Bluetooth packet structure **430** for the user's request includes the access code for the piconet master in the piconet formed by the mobile Bluetooth device and the Bluetooth access point, the header containing the slave device number and the packet type, and the payload portion. The payload portion includes the payload header and the payload data. The mobile wireless device receives the server response message. The mobile wireless device uses the information in the server response message to contact the server over the Internet to download

web pages or to conduct other server operations, reading on the claimed "A short-range wireless access point [apparatus] enabling a mobile wireless device to resume service with a network server after the wireless device moves out of the coverage area of the of the access point, comprising: a server including transceivers for short-range wireless communication within a coverage area and with a network server; means for registering [registration unit] the mobile device when initiating proximity services with a service provider; means for transmitting [transmitting unit] a code to the mobile device for identification purposes in short-range and network communications (*552*, fig. 2D); means for initiating a [initiating unit] session for the mobile device with the service provider when within the coverage area; and means for maintaining [maintaining unit] the session with the service provider when the mobile device moves outside the coverage area," (paragraphs 20, 22, 55).

However, Heinonen et al. fail to specifically disclose that that the second code is the wide area identification of the mobile device and is coupled to the first code.

In the same field of endeavor, Hasty, Jr. et al. clearly show and disclose that when the local IP stack on anode attempts to deliver a directed packet, it will first issue an ARP request to determine a MAC to IP address mapping (col. 6 line 35-55). Node **120** has a MAC address of 00:21:23:34:45:67. The MAC address of node **120** is subjected to a hashing function, which results in a two byte address of 98.34. This two byte address is appended to the two bytes of the

class B address to determine a node **120** IP address of 169.254.98.34. Each node of the ad-hoc routing network 100 periodically advertises via one or more routing advertisements (RA), each MAC address of destination nodes to which it can forward traffic, as well as the path through the network used to reach each destination; adds the two bytes of the unique IP address of the node to the routing advertisements so each contains both the MAC address and a sufficient IP address to successfully perform a mapping between the two, reading on the claimed "means for obtaining [obtaining unit] from the mobile device a wide area identification (MAC address) of the mobile device, wherein the code (class B address) and the wide area identification are to be coupled into a hashed code for proximity identification of the mobile device," (col. 5 line 25- col. line 25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the MAC address and the Class B address of the node to create an IP address as taught by Hasty, Jr. et al. in the system of Heinonen et al., in order to provide broadcast service from a network server.

However, Heinonen et al., as modified by Hasty, Jr. et al., fail to specifically disclose that a hash code is sent from a server to the mobile station and from the mobile station to another server.

In the same field of endeavor, Norefors et al. clearly show and disclose a method for achieving a secure handover of a mobile terminal from a first access point to a second access point. The method and/or network involves transmitting

a first message from the first access point to the mobile terminal over a radio interface, the first message containing an encrypted security token and a hash code. Thereafter, a message is transmitted from the mobile terminal to the second access point, this second message containing the re-encrypted security token and the hash code, reading on the claimed "wherein the hashed code is to be transmitted to the mobile device along with an instruction to forward the hashed code to the network server to associate the code and the wide area identification in a subsequent request for service by the mobile device," (col. 2 lines 16-38).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to transmit a hashed code to a new AP that was forwarded from an old AP as taught by Norefors et al. in the system of Heinonen et al., as modified by Hasty, Jr. et al., in order to provide a secure handover of service.

Consider **claims 2 and 41**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 1 and 40 above**, respectively, and in addition, Heinonen et al. further disclose that if the mobile wireless device detects that it has left the coverage area of the short range wireless access point while in contact with the server, it will determine whether the global/local parameter indicates that the service is global. If the parameter is global, then the mobile wireless device stores a bookmark of the server's URL, for example the URL and

path name for one of the prior web pages downloaded from the server. The mobile wireless device displays a notice to the user offering the user the option of continuing the contact with the server over the regional cellular telephone network, reading on the claimed "means for transferring the session to the network server when the mobile device moves outside the coverage area," (paragraph 21).

Consider **claims 4 and 42**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 1 and 40 above**, respectively, and in addition, Heinonen et al. further disclose that the short range wireless access point receives a response message over the Internet from the server, including a global/local parameter, reading on the claimed "means for coupling the access point to the service provider via an information network," (paragraph 20).

Consider **claims 7 and 43**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 1 and 40 above**, respectively, and in addition, Heinonen et al. further disclose that the access point forwards the response message to the mobile wireless device, which uses the information in the message to contact the server over the Internet to download web pages or to conduct other server operations. If the mobile wireless device detects that it has left the coverage area of the short range wireless access point while in contact with the server, it will determine whether the global/local parameter indicates that

the service is global. If the parameter is global, then the mobile wireless device stores a bookmark of the server's URL, for example the URL and path name for one of the prior web pages downloaded from the server. The mobile wireless device displays a notice to the user offering the user the option of continuing the contact with the server over the regional cellular telephone network, reading on the claimed "a service provider incorporated within the access point; and means for enabling the access point to contact the mobile device and provide services via the short-range communication link when the mobile device is within the coverage area or through a cellular network if the mobile device is outside the coverage area," (paragraphs 20, 21).

Consider **claims 8 and 44**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **applied to claims 1 and 40 above**, respectively, and in addition, Hasty, Jr. et al. further discloses that the MAC address of node **120** is subjected to a hashing function, which results in a two byte address of 98.34, reading on the claimed "the code is a MAC address and the wide area identification is a machine number for the mobile device," (col. 5 lines 64-66).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to hash the MAC address to create the IP address as taught by Hasty, Jr. et al. in the system of Heinonen et al., in order to provide broadcast service from a network server.

Consider **claims 9 and 45**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 1 and 40 above**, respectively, and in addition, Heinonen et al. further disclose that when the mobile wireless device is within the coverage area of the short range wireless access point, it sends a request for service to be obtained, over the Internet **144** from network server **180**. The short range wireless access point is a Bluetooth access point and the short range wireless circuits in the mobile wireless device are Bluetooth circuits, reading on the claimed "short-range communication link implements Bluetooth protocols," (paragraph 50).

Consider **claims 10 and 46**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 1 and 40 above**, respectively, Heinonen et al. further disclose that if the user selects to continue the contact with the server, then a stored handover address is accessed. The stored handover address may be a default address or alternately, it may be a handover address included in the prior response message from the server. The handover address will typically be the telephone number of a protocol gateway, such as a WAP gateway, connected between the cellular telephone network and the Internet. A cellular telephone connection is made by the mobile wireless device with the regional cellular telephone access point. Then, a cellular telephone call is placed to the protocol gateway. When the call is completed over the telephone network

from the mobile wireless device to the protocol gateway, the mobile wireless device sends a message to the protocol gateway, reading on the claimed "network server implements cellular protocols," (paragraph 22).

Consider **claims 11 and 47**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claim 4 and 42 above**, respectively, Heinonen et al. further disclose that the short range wireless access point receives a response message over the Internet from the server, including a global/local parameter, reading on the claimed "information network is the Internet," (paragraph 20).

Consider **claim 12**, Heinonen et al. clearly show and disclose that a user device receives a paging packet **530** from an access point (AP), reading on the claimed "short-range wireless access point," device. The user device's, reading on the claimed "mobile device," L2CAP layer **220** determines if the class of device (CoD) field **542** in the paging packet indicates that the next packet is an Access Point Service Indication (APSI) message **550**. If it is, then when the user's device receives the next packet(s) from the AP, the L2CAP layer loads it into an APSI message buffer. The L2CAP layer verifies that packet header indicates an APSI message from the AP. The user selectively enters an input to the GUI **234** to establish a connection with the AP, reading on the claimed "method in a short-range wireless access point for enabling a mobile device to resume service with a network server, the service having been interrupted by

moving the mobile device out of the coverage area of the access point, comprising; establishing a short-range communication link for initiating a service with the mobile wireless device, wherein the short-range communication link is based on a first local area identification of the mobile wireless device," for a session with the service platform server **180**, reading on the claimed "network server." The user device and the AP then open an SDP and/or a non-SDP channel and they begin a session. The AP registers the user's device with the service platform server and requests service for the user's device. Then, the user's device and the service platform server conduct a session via the AP, reading on the claimed "determining whether the service with the mobile wireless device through the short-range communication link is open," (paragraphs 85-93). If the mobile wireless device detects that it has left the coverage area of the short range wireless access point while in contact with the server, it will determine whether a global/local parameter indicates that the service is global. If the parameter is global, then the mobile wireless device may store a bookmark of the server's URL. The mobile wireless device displays a notice on browser **102** to the user, offering the user the option of continuing the contact with the server over the regional cellular telephone network. If the user selects to continue the contact with the server 180, then a stored handover address **582** is accessed. The handover address 582 may be stored in the mobile wireless device. The handover address will typically be the telephone number of a protocol gateway **118**, such as a WAP gateway, connected between the cellular telephone network

116 and the Internet **144**. A cellular telephone connection is made by the mobile wireless device 100 with the regional cellular telephone access point. Then, a cellular telephone call is placed to the protocol gateway. When the call is completed over the telephone network from the mobile wireless device to the protocol gateway, the mobile wireless device sends a message to the protocol gateway, which it forwards to the server. Depending on the request, the server responds by resuming the operations it had previously been conducting in its prior contact with the mobile wireless device, reading on the claimed "establishing wide area connection with the mobile wireless device using a stored association in response to detecting that the short-range communication link is closed," (paragraph 94). The Bluetooth access point forwards the response message **435** to the user's Bluetooth device from the server. The Bluetooth packet structure **430** for the user's request includes the access code for the piconet master in the piconet formed by the mobile Bluetooth device and the Bluetooth access point, the header containing the slave device number and the packet type, and the payload portion. The payload portion includes the payload header and the payload data. The mobile wireless device receives the server response message. The mobile wireless device uses the information in the server response message to contact the server over the Internet to download web pages or to conduct other server operations, reading on the claimed "transmitting a message to the mobile device and instructing the mobile device to forward the message to the server for associating the first identification with the

second identification in a subsequent request for service by the mobile device," (paragraph 55).

However, Heinonen et al. fail to specifically disclose that that the second code is the wide area identification of the mobile device and is coupled to the first code.

In the same field of endeavor, Hasty, Jr. et al. clearly show and disclose that when the local IP stack on anode attempts to deliver a directed packet, it will first issue an ARP request to determine a MAC to IP address mapping (col. 6 line 35-55). Node **120** has a MAC address of 00:21:23:34:45:67. The MAC address of node **120** is subjected to a hashing function, which results in a two byte address of 98.34. This two byte address is appended to the two bytes of the class B address to determine a node **120** IP address of 169.254.98.34. Each node of the ad-hoc routing network 100 periodically advertises via one or more routing advertisements (RA), each MAC address of destination nodes to which it can forward traffic, as well as the path through the network used to reach each destination; adds the two bytes of the unique IP address of the node to the routing advertisements so each contains both the MAC address and a sufficient IP address to successfully perform a mapping between the two, reading on the claimed "requesting from the mobile wireless device a second identification through the short-range communication link; receiving the additional identification from the mobile wireless device; wherein the requested identification relates to a wide area network identification of the terminal; coupling the first and second

identifications in a hashed code as a proximity identification of the mobile device," (col. 5 line 25- col. line 25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the MAC address and the Class B address of the node to create an IP address as taught by Hasty, Jr. et al. in the system of Heinonen et al., in order to provide broadcast service from a network server.

However, Heinonen et al., as modified by Hasty, Jr. et al., fail to specifically disclose that a hash code is sent from an access point to the mobile station and from the mobile station to another server.

In the same field of endeavor, Norefors et al. clearly show and disclose a method for achieving a secure handover of a mobile terminal from a first access point to a second access point. The method and/or network involves transmitting a first message from the first access point to the mobile terminal over a radio interface, the first message containing an encrypted security token and a hash code. Thereafter, a message is transmitted from the mobile terminal to the second access point, this second message containing the re-encrypted security token and the hash code, reading on the claimed "transmitting a message to the mobile device including the hashed code and instructing the mobile device to forward the message to the server for associating the first identification with the second identification in a subsequent request for service by the mobile device," (col. 2 lines 16-38).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to transmit a hashed code to a new AP that was forwarded from an old AP as taught by Norefors et al. in the system of Heinonen et al., as modified by Hasty, Jr. et al., in order to provide a secure handover of service.

Consider **claim 13**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claim 12 above**, Heinonen et al. further disclose that when the user's device **100** sends either a paging packet or an inquiry response packet, such as inquiry response packet **510**, to the access point **140**, the access point uses the information in the received packet as stimuli to be matched with trigger words stored in the trigger word table **260**. For example, the address of the device in field **520** can be matched with address values **266** in the trigger word table. Also, the class of device of the device in field **522** can be compared with class of device values **268** stored in the trigger word table, reading on the claimed "providing the access point with the first and the second identification of the mobile device," (paragraph 80).

Consider **claim 14**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claim 12 above**, Heinonen et al. further disclose that the short range wireless access point receives a response message over the Internet from the server, including a global/local parameter, reading on the claimed

"coupling the access point to the service provider via an information network," (paragraph 20).

Consider **claim 17**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claim 12 above**, Heinonen et al. further disclose that the access point forwards the response message to the mobile wireless device, which uses the information in the message to contact the server over the Internet to download web pages or to conduct other server operations. If the mobile wireless device detects that it has left the coverage area of the short range wireless access point while in contact with the server, it will determine whether the global/local parameter indicates that the service is global. If the parameter is global, then the mobile wireless device stores a bookmark of the server's URL, for example the URL and path name for one of the prior web pages downloaded from the server. The mobile wireless device displays a notice to the user offering the user the option of continuing the contact with the server over the regional cellular telephone network, reading on the claimed "incorporating a service provider within the access point; and enabling the access point to contact the mobile device and provide services via the short-range communication link when the mobile device is within the coverage area or through a cellular network if the mobile device is outside the coverage area," (paragraphs 20, 21).

Consider **claim 18**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed

invention **applied to claim 13 above**, and in addition, Hasty, Jr. et al. further discloses that the MAC address of node **120** is subjected to a hashing function, which results in a two byte address of 98.34, reading on the claimed "the code is a MAC address and the wide area identification is a machine number for the mobile device," (col. 5 lines 64-66).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to hash the MAC address to create the IP address as taught by Hasty, Jr. et al. in the system of Heinonen et al., in order to provide broadcast service from a network server.

Consider **claim 19**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claim 12 above**, Heinonen et al. further disclose that when the mobile wireless device is within the coverage area of the short range wireless access point, it sends a request for service to be obtained, over the Internet **144** from network server **180**. The short range wireless access point is a Bluetooth access point and the short range wireless circuits in the mobile wireless device are Bluetooth circuits, reading on the claimed "short-range communication link implements Bluetooth protocols," (paragraph 50).

Consider **claim 20**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claim 12 above**, Heinonen et al. further disclose that if the user selects to continue the contact with the server, then a stored handover

address is accessed. The stored handover address may be a default address or alternately, it may be a handover address included in the prior response message from the server. The handover address will typically be the telephone number of a protocol gateway, such as a WAP gateway, connected between the cellular telephone network and the Internet. A cellular telephone connection is made by the mobile wireless device with the regional cellular telephone access point. Then, a cellular telephone call is placed to the protocol gateway. When the call is completed over the telephone network from the mobile wireless device to the protocol gateway, the mobile wireless device sends a message to the protocol gateway, reading on the claimed "network server implements cellular protocols in establishing a wide area connection," (paragraph 22).

Consider **claim 21**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claim 14 above**, Heinonen et al. further disclose that the short range wireless access point receives a response message over the Internet from the server, including a global/local parameter, reading on the claimed "information network is the Internet," (paragraph 20).

Consider **claims 22, 31 and 48**, Heinonen et al. clearly show and disclose that during the period when a mobile wireless device, reading on the claimed "wireless device," is within the coverage area of a short range wireless access point, reading on the claimed "hotspot server," it sends a request for service to be obtained over the Internet from a network server. The short range wireless

access point forwards that request over the Internet to the server, augmented with additional information including the network address and geographic location of the access point. The short range wireless access point receives a response message over the Internet from the server, including a global/local parameter. The global/local parameter, reading on the claimed "code for identification purposes in short-range and network communications," will notify the mobile wireless device whether the requested service is available outside the coverage area of the short range wireless access point. The access point forwards the response message to the mobile wireless device, which uses the information in the message to contact the server over the Internet to download web pages or to conduct other server operations. If the user selects to continue the contact with the server, then a stored handover address is accessed. The handover address may be stored in the mobile wireless device or alternately, it may be stored in the short range wireless access point. A cellular telephone connection is made by the mobile wireless device with the regional cellular telephone access point, reading on the claimed "A system [apparatus] enabling a mobile wireless device to resume service with a network server after the wireless device moves out of a coverage area of an access point, comprising: a hotspot server including transceivers for short-range wireless communication within a coverage area and with a network server; a mobile device including means for short-range communication and network communications; means for coupling [coupling unit] the hotspot server to a service provider; means [unit] stored in the mobile device

for implementing short-range communications with the hotspot server when within the coverage area; means [unit] stored in the hotspot server for recognizing the mobile device when initiating short-range communication with the mobile device; means for registering [registration unit] the mobile device when initiating proximity services with the service provider; means initiating [initiation unit] a session for the mobile device with the service provider within the coverage area; means maintaining [maintaining unit] the session with the service provider using the code when the mobile device moves outside the coverage area," (paragraphs 20, 22). The Bluetooth access point forwards the response message **435** to the user's Bluetooth device from the server. The Bluetooth packet structure **430** for the user's request includes the access code for the piconet master in the piconet formed by the mobile Bluetooth device and the Bluetooth access point, the header containing the slave device number and the packet type, and the payload portion. The payload portion includes the payload header and the payload data. The mobile wireless device receives the server response message. The mobile wireless device uses the information in the server response message to contact the server over the Internet to download web pages or to conduct other server operations, reading on the claimed "means for transmitting [transmitting unit] a code and a message to the mobile device for identification purposes in short-range and network communications, wherein the message comprises an instruction to the mobile device to send the code to the

service provider to associate the first and second identities fro a subsequent request for service," (paragraph 55).

However, Heinonen et al. fail to specifically disclose that that the second code is the wide area identification of the mobile device and is coupled to the first code.

In the same field of endeavor, Hasty, Jr. et al. clearly show and disclose that when the local IP stack on anode attempts to deliver a directed packet, it will first issue an ARP request to determine a MAC to IP address mapping (col. 6 line 35-55). Node **120** has a MAC address of 00:21:23:34:45:67. The MAC address of node **120** is subjected to a hashing function, which results in a two byte address of 98.34. This two byte address is appended to the two bytes of the class B address to determine a node **120** IP address of 169.254.98.34. Each node of the ad-hoc routing network 100 periodically advertises via one or more routing advertisements (RA), each MAC address of destination nodes to which it can forward traffic, as well as the path through the network used to reach each destination; adds the two bytes of the unique IP address of the node to the routing advertisements so each contains both the MAC address and a sufficient IP address to successfully perform a mapping between the two, reading on the claimed "said means for registering [registration unit] to obtain and request first, local and second, network identifiers associated with the mobile device; wherein the requested identification relates to a wide area network identification of the

terminal; wherein the code comprises a hashed coded formed from the first and second identifiers," (col. 5 line 25- col. line 25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the MAC address and the Class B address of the node to create an IP address as taught by Hasty, Jr. et al. in the system of Heinonen et al., in order to provide broadcast service from a network server.

However, Heinonen et al., as modified by Hasty, Jr. et al., fail to specifically disclose that a hash code is sent from an access point to the mobile station and from the mobile station to another server.

In the same field of endeavor, Norefors et al. clearly show and disclose a method for achieving a secure handover of a mobile terminal from a first access point to a second access point. The method and/or network involves transmitting a first message from the first access point to the mobile terminal over a radio interface, the first message containing an encrypted security token and a hash code. Thereafter, a message is transmitted from the mobile terminal to the second access point, this second message containing the re-encrypted security token and the hash code, reading on the claimed "means for transmitting [transmitting unit] a code and a message to the mobile device for identification purposes in short-range and network communications, wherein the message comprises an instruction to the mobile device to send the code to the service

provider to associate the first and second identifiers for a subsequent request for service," (col. 2 lines 16-38).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to transmit a hashed code to a new AP that was forwarded from an old AP as taught by Norefors et al. in the system of Heinonen et al., as modified by Hasty, Jr. et al., in order to provide a secure handover of service.

Consider **claims 23, 32 and 49**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 22, 31 and 48 above**, respectively, and in addition, Hasty, Jr. et al. further discloses that one possible way to provide an automatic domain name is to combine the IOT serial number with the last two digits of the MAC address. Other combinations of readily available information known to the user and the CS Platform by default are possible, reading on the claimed "means coupling a MAC address and a cellular address number of the mobile device in a code as an identificator of a subscriber of proximity services," (paragraph 194).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the serial number and MAC address to create a unique domain name as taught by Hasty, Jr. et al. in the system of Heinonen et al., in order to provide service from a network server.

Consider **claims 24, 33 and 50**, Heinonen et al., as modified by Hasty, Jr. et al., clearly show and disclose the claimed invention **as applied to claims 22, 31 and 48 above**, respectively, and in addition, Heinonen et al. further disclose that the user selectively enters an input to the GUI to establish a connection with the AP for a session with the service platform server, reading on the claimed "backend server." The user device and the AP then open an SDP and/or a non-SDP channel and they begin a session. The AP registers the user's device with the service platform server and requests service for the user's device. Then, the user's device and the service platform server conduct a session via the AP, reading on the claimed "hotspot server is coupled to a backend server," (paragraphs 91-93).

Consider **claims 25, 34 and 51**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 22, 31 and 48 above**, respectively, and in addition, Heinonen et al. further disclose that during an initial period when the mobile wireless device is within the coverage area of the short range wireless access point, it sends a request for service to be obtained, for example, over the Internet from network server. The Bluetooth access point forwards the user's service request in an augmented service request message to the server 180. The service request from the user's device is forwarded by the access point in the augmented service request message, over, for example, the LAN **142** and the Internet **144** to the content server, reading on the claimed "service provider is

incorporated within the hotspot server and the server selects a first communication protocol to link with the mobile device when the mobile device is within the coverage area and a second communication protocol as a smooth handover when the mobile device leaves the coverage area," (paragraph 50, 52).

Consider **claims 26, 35 and 52**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 22, 35 and 48 above**, respectively, and in addition, Heinonen et al. further disclose that if the mobile wireless device detects that it has left the coverage area of the short range wireless access point while in contact with the server, it will determine whether a global/local parameter indicates that the service is global. If the parameter is global, then the mobile wireless device may store a bookmark of the server's URL. The mobile wireless device displays a notice on browser to the user, offering the user the option of continuing the contact with the server over the regional cellular telephone network. If the user selects to continue the contact with the server 180, then a stored handover address is accessed. The handover address 582 may be stored in the mobile wireless device. The handover address will typically be the telephone number of a protocol gateway, such as a WAP gateway, connected between the cellular telephone network and the Internet. A cellular telephone connection is made by the mobile wireless device with the regional cellular telephone access point. Then, a cellular telephone call is placed to the protocol gateway. When the call is completed over the telephone network from the

mobile wireless device to the protocol gateway, the mobile wireless device sends a message to the protocol gateway, which it forwards to the server. Depending on the request, the server responds by resuming the operations it had previously been conducting in its prior contact with the mobile wireless device, reading on the claimed "provider continues a consumer relation with the mobile device while out of the coverage area using the cellular address number of the device," (paragraph 94).

Consider **claims 28, 37 and 54**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 22, 31 and 48 above**, respectively, and in addition, Heinonen et al. further disclose that the AP registers the user's device with the service platform server and requests service for the user's device. Then, the user's device and the service platform server conduct a session via the AP. The service platform server can then download the maps, advertising and/or other service offerings to the mobile Bluetooth device, reading on the claimed "service provider provides tailored services to a mobile device," (paragraph 93).

Consider **claims 30, 39 and 56**, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention **as applied to claims 22, 31 and 48 above**, respectively, and in addition, Heinonen et al. further disclose that the server responds by resuming the operations it had previously been conducting in its prior contact with the mobile wireless device. For example, WML, HTML, or graphics files can be

returned by the server to the WAP gateway. For example, the server can respond to a GET method request by sending the requested web page to the protocol gateway. Alternately, the server can respond by executing CGI, ASP, or JSP scripts or other server programs to dynamically generate WML or HTML content to be returned to the WAP gateway. The protocol gateway then performs an HTML to WML conversion of the content, followed by WML encoding to form the WSP response message. The WSP response message is then transmitted by the WAP gateway over the telephone network to the cellular telephone access device. The cellular telephone access device then transmits the WSP response message containing the content, over the cellular telephone air link to the mobile wireless device, reading on the claimed "service provider services are browser/J2ME based," (paragraph 24).

4. **Claims 27, 36 and 53** are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of **Heinonen et al. (U.S. 2003/0112789 A1)** and **Hasty, Jr. et al. (US 6,728,232 B2)** in view of **Norefors et al. (US 6,370,380 B1)**, and in further view of **Bjorklund et al. (U.S. 2003/0046184)**.

Consider **claims 27, 36 and 53**, and **as applied to claims 22, 31 and 48 above**, respectively, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention except that the network server provides SMS/MMS based service.

In the same field of endeavor, Bjorklund et al. clearly show and disclose a digital pen that communicates with an application service provider to perform a desired function. The digital pen **104** may be associated with an individual or business end user. End users may utilize the digital pen and digital paper for a variety of purposes. For example, writing from a digital pen on digital paper may be transformed to a facsimile message, an electronic mail (e-mail) message, or a short message (e.g., SMS-short message service). The pen may be hard wired, provided with infrared base communication technology or may communicate to a communication channel for eventual transfer to the desired destination via a pen-communication channel connection **112** which may desirably employ wireless data transmission utilizing the Bluetooth communication protocol. The digital pen communicates information via a Bluetooth encoded wireless transmission, to a Bluetooth enabled wireless telephone or PDA (personal digital assistant) which may save the data and then, in turn, transmit the data to a personal computer connected to a communications network such as the internet, (paragraphs 32, 33). A technological service provider **120** verifies that the pen user is an authorized user with a current account and then sends the pen of the pen user the address of the application service provider **200**, in this case an SMS server, reading on the claimed "services provider services are SMS/MMS based," (paragraph 44).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide an end-user in a Bluetooth

environment with SMS services as taught by Bjorklund et al. in the system of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., in order to provide service from a network server.

5. **Claims 29, 38 and 55** are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of **Heinonen et al. (U.S. 2003/0112789 A1)** and **Hasty, Jr. et al. (US 6,728,232 B2)** in view of **Norefors et al. (US 6,370,380 B1)**, and in further view of **Belmont (U.S. 2004/0127204)**.

Consider **claims 29, 38 and 55**, and **as applied to claims 22, 31 and 48 above**, respectively, the combination of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., clearly show and disclose the claimed invention except that the billing data is sent to the mobile device in a SMS message.

In the same field of endeavor, Belmont clearly shows and discloses that a user of MU **100** sends a SMS/MMS "connect me" message to the cell phone whose number is shown on the display at public AP **300**. The message may be received by public AP configuration server **310**, and in response, configuration server may begin to exchange configuration information with MU by sending SMS/MMS messages. The public AP may send SMS/MMS messages or may use a secured LAN connection to the cellular operator to provide the costs, billing information and terms of a required WLAN service (step 640), reading on the claimed "access point tracks and calculates services used by a mobile device

within a billing zone and sends the billing data to the mobile device in a SMS message," (fig. 3, paragraphs 31, 34).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send billing information to a mobile unit via SMS as taught by Belmont in the system of Heinonen et al. and Hasty, Jr. et al., as modified by Norefors et al., in order to provide service from a network server.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAIME M. HOLLIDAY whose telephone number is

(571)272-8618. The examiner can normally be reached on Monday through Friday 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Appiah can be reached on (571) 272-7904. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jaime M Holliday/
Examiner, Art Unit 2617

/Charles N. Appiah/
Supervisory Patent Examiner, Art Unit 2617